

1/10

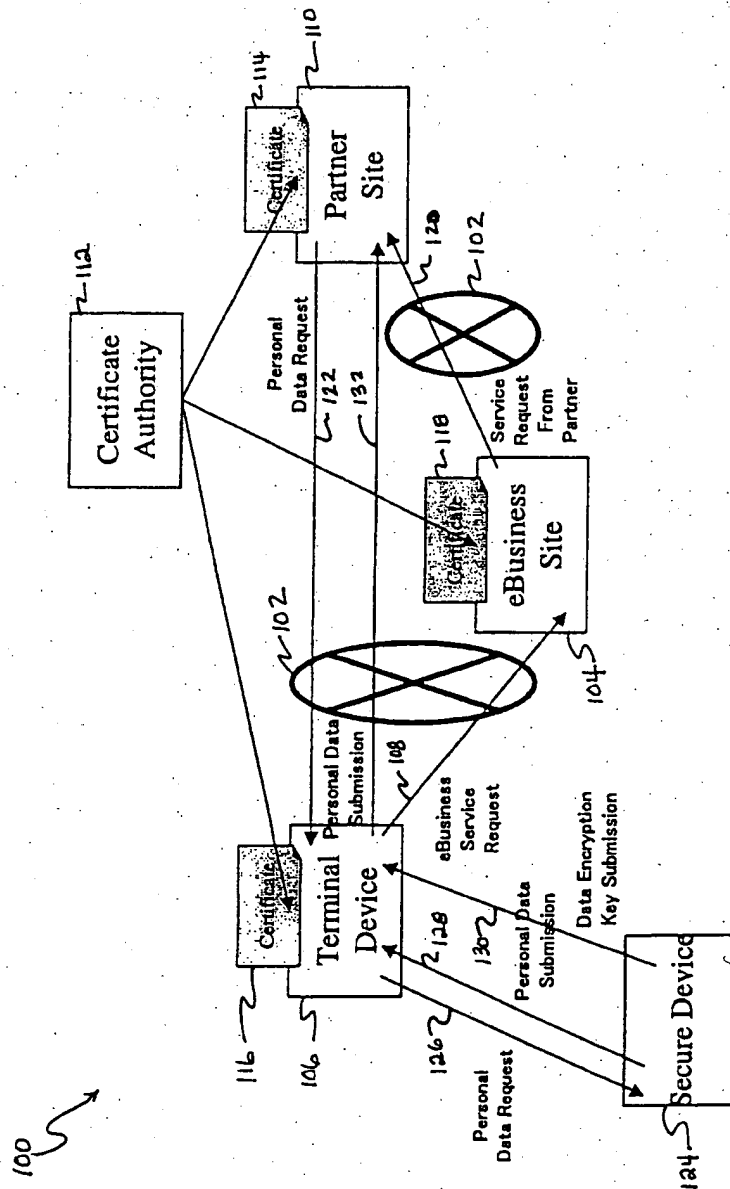


FIG. 1

2/10

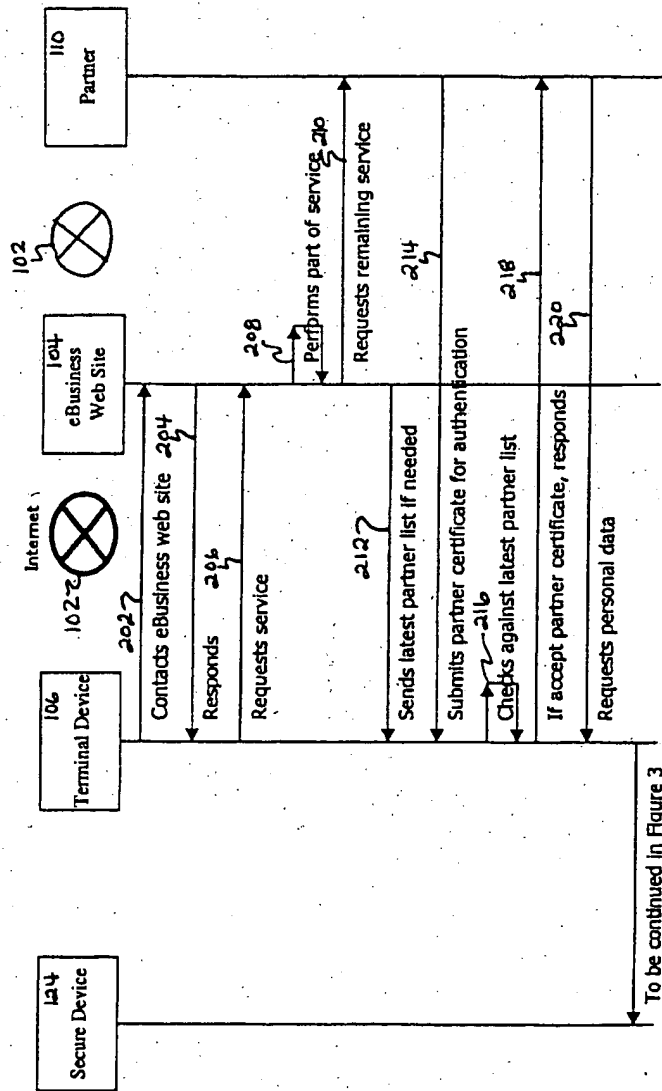


FIG. 2

3/10

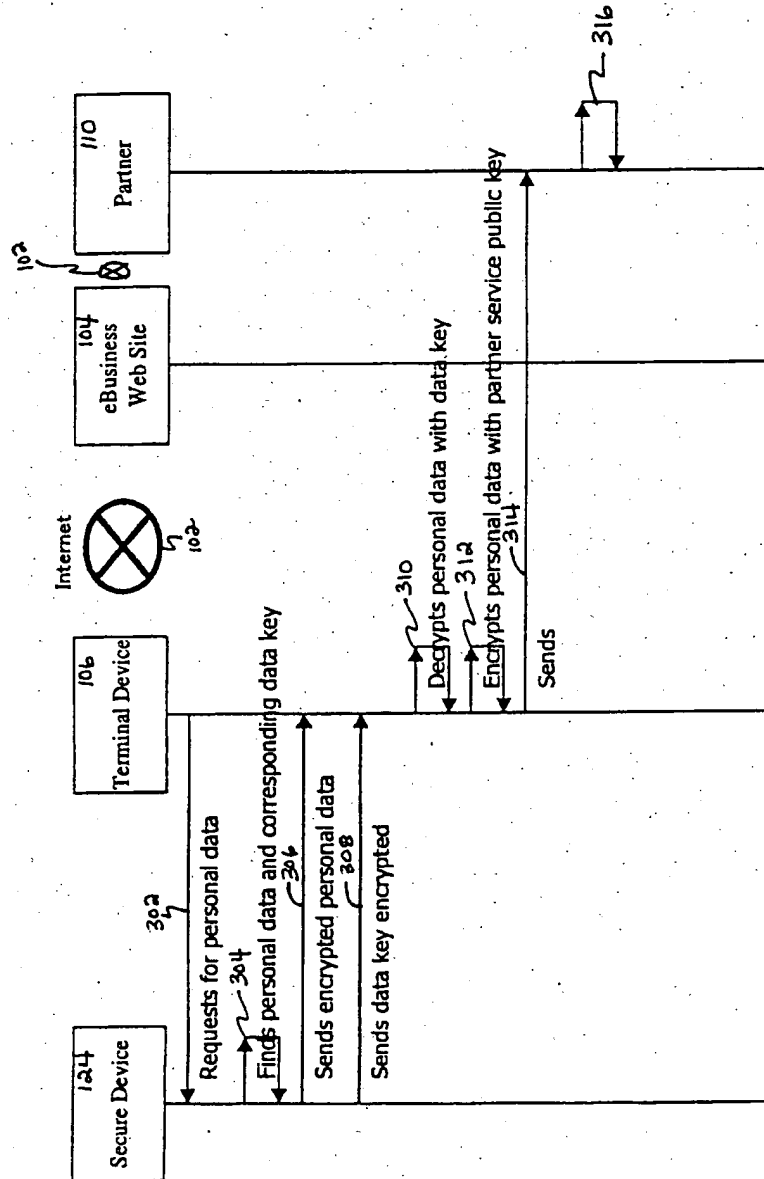


FIG. 3

4/10

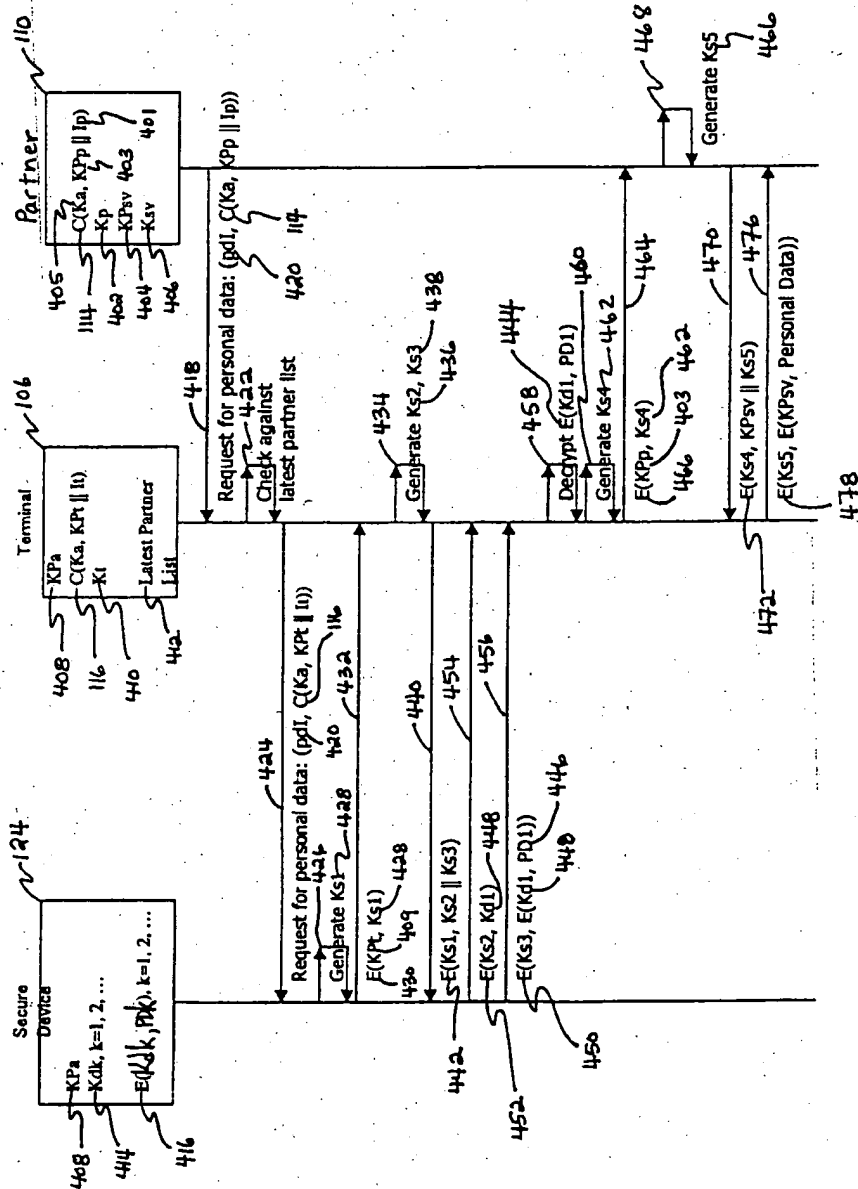


FIG. 4

Name	Expression	Description
Encryption	$E(K, D)$	The result of encrypting information "D" with key "K"
Hash	$H(D)$	The result of hashing information "D"
Concatenation	$A \parallel B$	Concatenation of "A" and "B"
CA Private Key	$K_a$	A private key used by a CA to sign certificate
CA Public Key	$KP_a$	A public key corresponding to $K_a$
Partner Information	$I_p$	The information pertaining to the partner
Partner Private Key	$K_p$	A private key owned by the partner
Partner Public Key	$KP_p$	A public key corresponding to $K_p$
Partner Certificate	$C(K_a, KP_p \parallel I_p)$	X.509 certificate for the partner
Partner Service Private Key	$K_{sv}$	A private key owned by the partner service
Partner Service Public Key	$KP_{sv}$	A public key corresponding to $K_{sv}$
Terminal Information	$I_t$	The information pertaining to the partner
Terminal Private Key	$K_t$	A private key owned by the terminal
Terminal Public Key	$KP_t$	A public key corresponding to $K_t$
Terminal Certificate	$C(K_a, KP_t \parallel I_t)$	X.509 certificate for the terminal
Personal Data	$PDK, k=1, 2, \dots$	Personal data for eBusiness service transaction
Personal Data Encryption Key	$Kdk, k=1, 2, \dots$	A symmetric key to encrypt personal data (stored in the TRM of the PIN-SMMC)
Encrypted Personal Data	$E(PDK, Kdk), k=1, 2, \dots$	Personal data stored in an encrypted format in the flash memory portion of the PIN-SMMC
Personal Data information	$p d I$	Information related to identifying the appropriate personal data to submit to the partner site
Session Key	$Ksk, k=1, 2, \dots$	A symmetric key generated in real-time to encrypt a communication session

FIG. 5

6/10

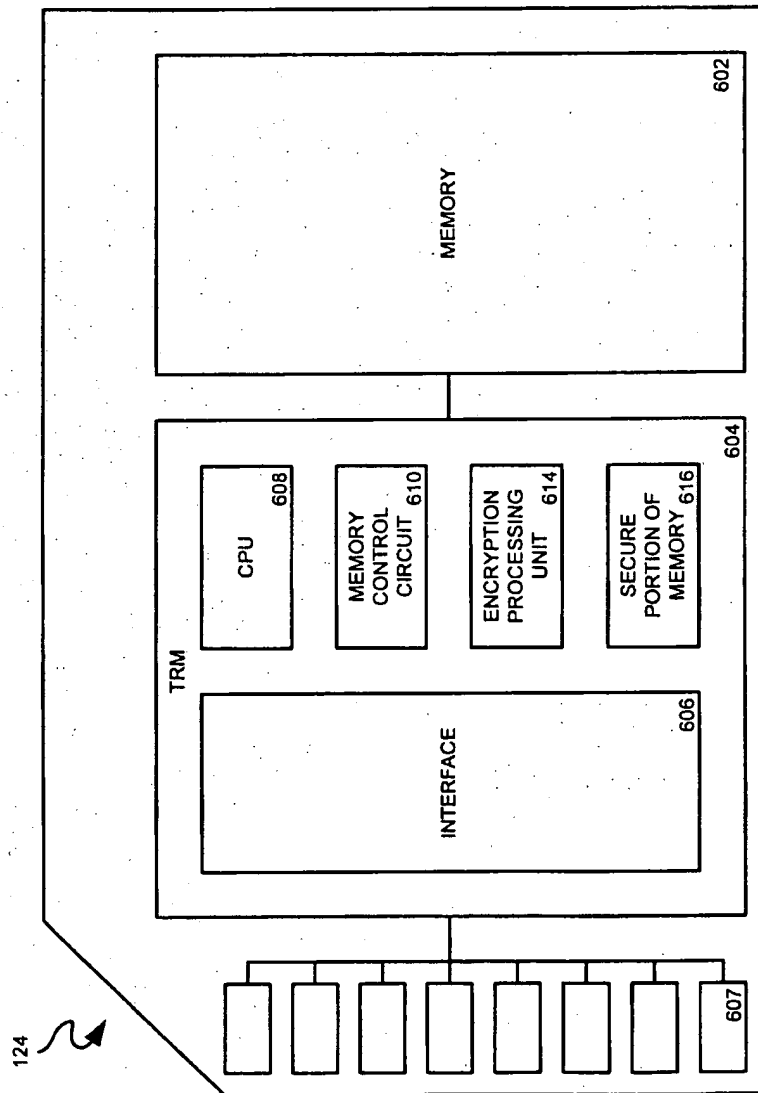


FIG. 6

7/10

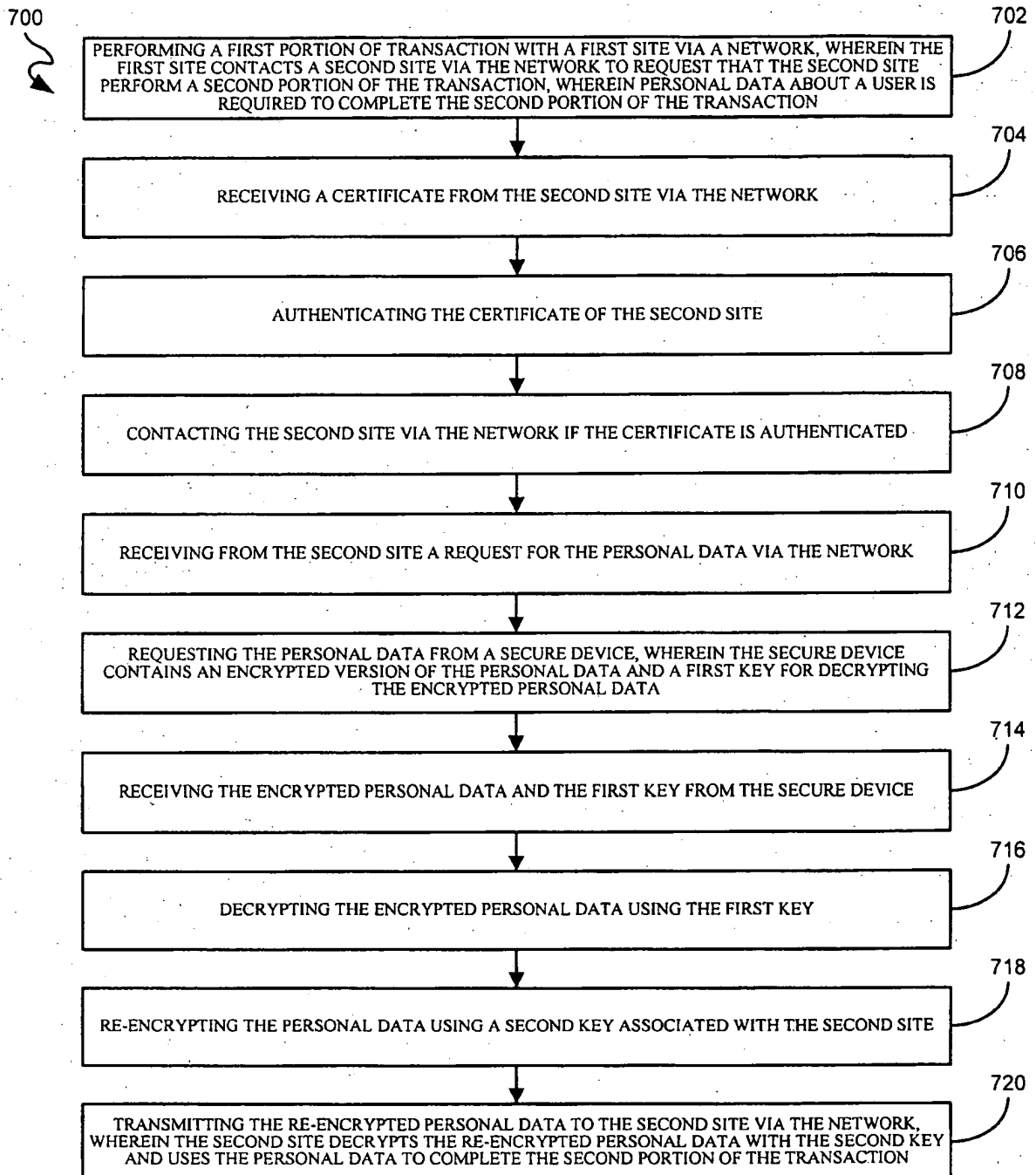


FIG. 7

8/10

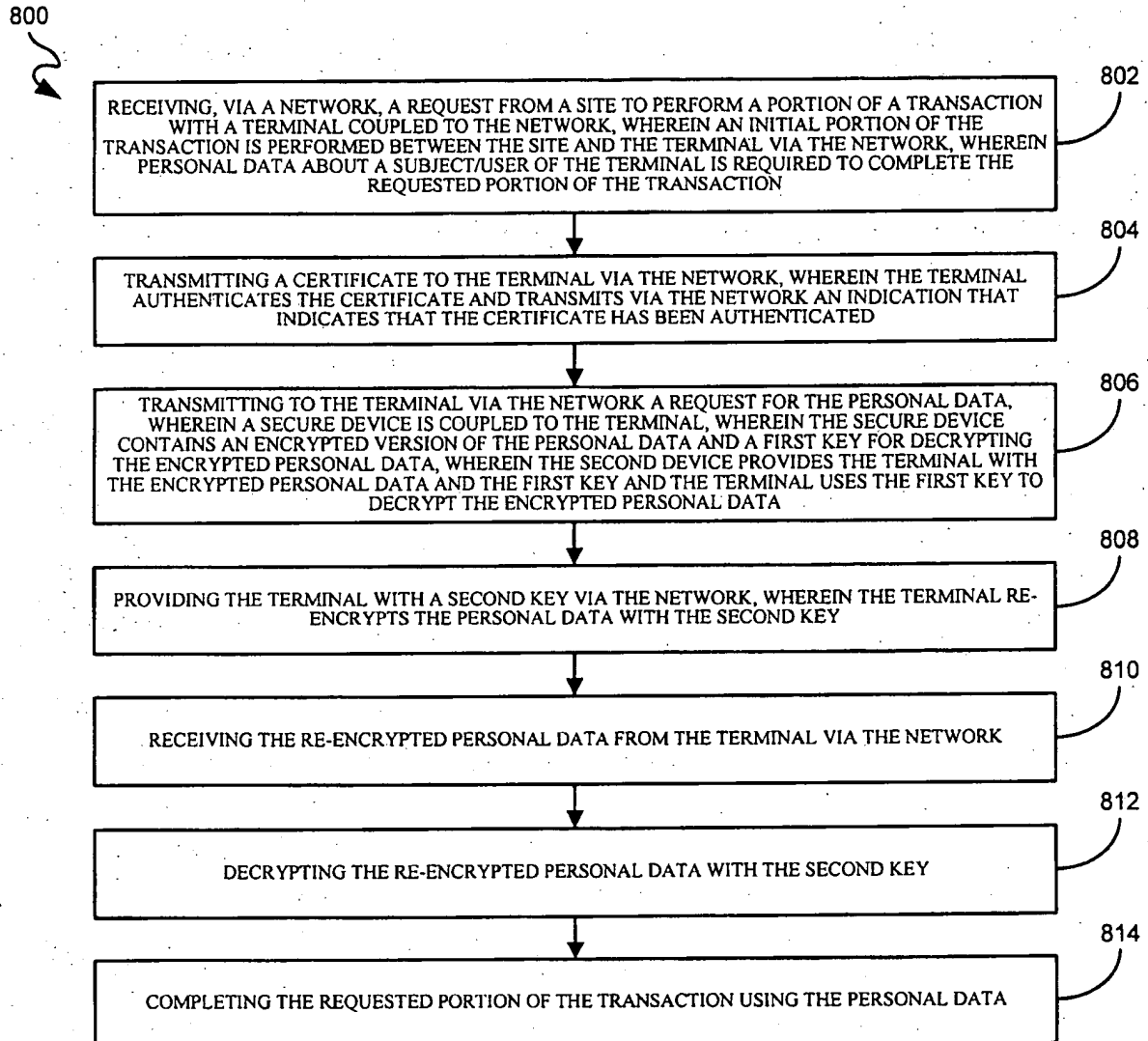


FIG. 8



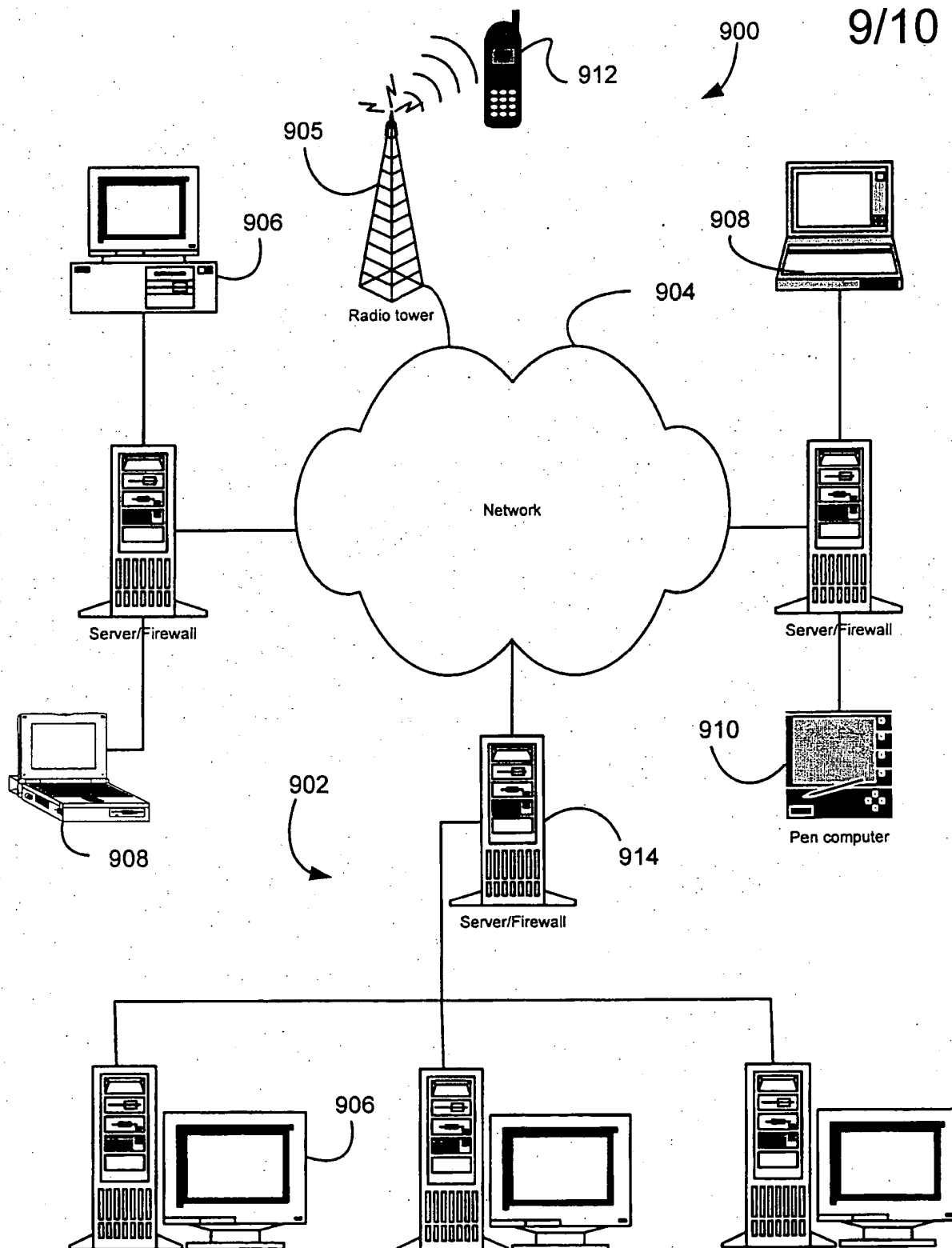


FIG. 9

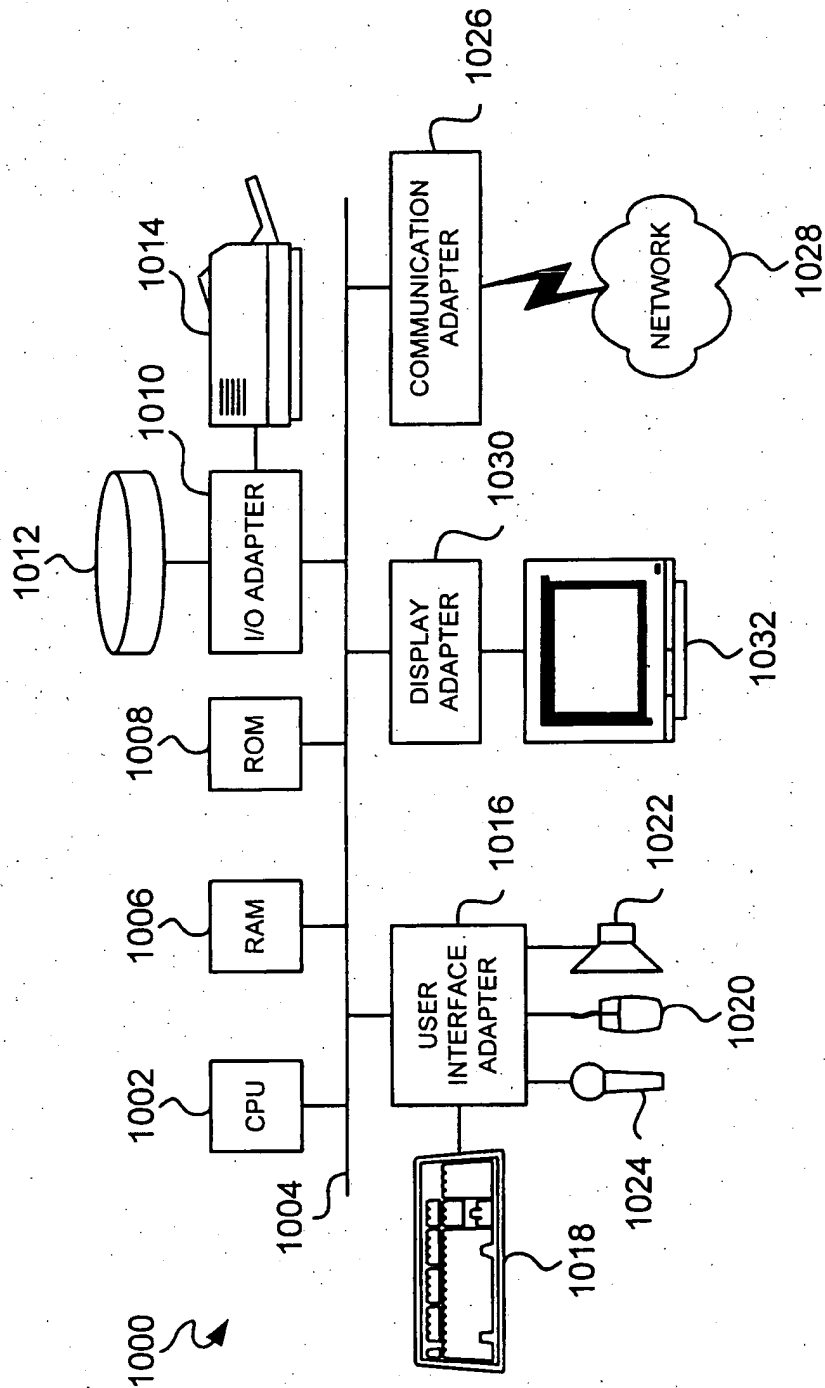


FIG. 10